

What is claimed is

1           1. An elliptic curve exponentiation apparatus that  
2     computes an elliptic curve exponentiation for an elliptic  
3     curve  $E: y^2 = x^3 + a \times x + b$  defined over a residue field  $F$  with a  
4     prime  $p$  being a modulus, comprising:

5           an information obtaining unit operable to obtain a point  
6      $Q$  that is on the elliptic curve  $E$ , and an exponent  $k$  that  
7     is a positive integer smaller than the prime  $p$ ;

8           a first storage unit operable to store therein a  
9     coefficient  $a$  that is an  $x$  term of the elliptic curve  $E$ ;

10          a computation unit operable to compute an elliptic curve  
11     exponentiation of the exponent  $k$  and the point  $Q$  using the  
12     coefficient  $a$  stored in the first storage unit, to obtain  
13     an exponentiation-result-point  $k \times Q$ ;

14          a judgment unit operable to judge whether the obtained  
15     exponentiation-result-point  $k \times Q$  is on the elliptic curve  $E$ ;

16     and

17          an output unit operable to output the obtained  
18     exponentiation-result-point  $k \times Q$ , when a judgment result of  
19     the judging unit is affirmative.

1           2. The elliptic curve exponentiation apparatus of Claim  
2     1, further comprising

3           a second storage unit operable to store therein a

4 coefficient  $b$  that is a constant term of the elliptic curve  
5  $E$ ,

6 wherein the judgment unit judges whether the obtained  
7 exponentiation-result-point  $k*Q$  is on the elliptic curve  $E$ ,  
8 using the coefficient  $a$  stored in the first storage unit and  
9 the coefficient  $b$  stored in the second storage unit.

1 3. The elliptic curve exponentiation apparatus of Claim  
2 2, further comprising

3 a constant term coefficient obtaining unit operable to  
4 obtain the coefficient  $b$ , and write the obtained coefficient  
5  $b$  into the second storage unit.

1 4. The elliptic curve exponentiation apparatus of Claim  
2 2, further comprising

3 an  $x$  term coefficient obtaining unit operable to obtain  
4 the coefficient  $a$ , and write the obtained coefficient  $a$  into  
5 the first storage unit.

1 5. The elliptic curve exponentiation apparatus of Claim  
2 2, further comprising

3 a constant term coefficient computation unit operable  
4 to compute the coefficient  $b$ , using the coefficient  $a$  stored  
5 in the first storage unit, the obtained point  $Q$ , and the elliptic  
6 curve  $E: y^2 = x^3 + a \times x + b$ , and write the computed coefficient  $b$  into

7 the second storage unit.

1 6. The elliptic curve exponentiation apparatus of Claim  
2 5, wherein

3 the computation unit computes coordinates  $(Qx, Qy)$  as  
4 the exponentiation-result-point  $k*Q$ , and

5 the judgment unit computes  $(Qy)^2$  and  $(Qx)^3+a*Qx+b$ ,  
6 compares a computation result of  $(Qy)^2$  and a computation result  
7 of  $(Qx)^3+a*Qx+b$ , and when the computation result of  $(Qy)^2$   
8 and the computation result of  $(Qx)^3+a*Qx+b$  match, judges that  
9 the exponentiation-result-point  $k*Q$  is on the elliptic curve  
10  $E$ .

1 7. The elliptic curve exponentiation apparatus of Claim  
2 5, further comprising

3 an error message output unit operable to output a message  
4 indicating that an error has occurred, when the judgment unit  
5 judges that the exponentiation-result-point  $k*Q$  is not on  
6 the elliptic curve  $E$ .

1 8. The elliptic curve exponentiation apparatus of Claim  
2 1, wherein

3 the judgment unit judges whether the point  $Q$  and the  
4 exponentiation-result-point  $k*Q$  are on a same elliptic curve,

5 instead of judging whether the exponentiation-result-point  
6  $k*Q$  is on the elliptic curve  $E$ , and  
7 the output unit outputs the exponentiation-result-point  
8  $k*Q$  when the judgment unit judges that the point  $Q$  and the  
9 exponentiation-result-point  $k*Q$  are on the same elliptic curve,  
10 instead of when the judgment unit judges that the  
11 exponentiation-result-point  $k*Q$  is on the elliptic curve  $E$ .

1 9. The elliptic curve exponentiation apparatus of Claim  
2 8, wherein  
3 the information obtaining unit obtains coordinates  $(Qx,$   
4  $Qy)$  as the point  $Q$ ,  
5 the computation unit computes coordinates  $(Qx', Qy')$   
6 as the exponentiation-result-point  $k*Q$ , and  
7 the judgment unit judges whether the point  $Q$  and the  
8 exponentiation-result-point  $k*Q$  are on the same elliptic  
9 curve, by judging whether  $(Qy^2 - Qx^3 - a \times Qx) - (Qy'^2 - Qx'^3 - a \times$   
10  $Qx') = 0$ .

1 10. An information security apparatus that ensures  
2 secure handling of predetermined information by computing  
3 an elliptic curve exponentiation of  $k*Q$ , based on  
4 computational complexity of solving a discrete logarithm  
5 problem on an elliptic curve  $E: y^2 = x^3 + a \times x + b$  defined over a  
6 residue field  $F$  with a prime  $p$  being a modulus, comprising:

7           an information obtaining unit operable to obtain a point  
8    $Q$  that is on the elliptic curve  $E$ , and an exponent  $k$  that  
9   is a positive integer smaller than the prime  $p$ ;  
10          a first storage unit operable to store therein a  
11   coefficient  $a$  that is an  $x$  term of the elliptic curve  $E$ ;  
12          a computation unit operable to compute an elliptic curve  
13   exponentiation of the exponent  $k$  and the point  $Q$  using the  
14   coefficient  $a$  stored in the first storage unit, to obtain  
15   an exponentiation-result-point  $k*Q$ ;  
16          a judgment unit operable to judge whether the obtained  
17   exponentiation-result-point  $k*Q$  is on the elliptic curve  $E$ ;  
18   and  
19          a prohibition unit operable to prohibit an output of  
20   the obtained exponentiation-result-point  $k*Q$ , when a  
21   judgment result of the judging unit is negative.

1           11. The information security apparatus of Claim 10,  
2   wherein

3           the elliptic curve exponentiation of  $k*Q$  is computed,  
4   to realize processes of: encryption of a plaintext, decryption  
5   of a ciphertext; generation of a signature for a plaintext;  
6   signature verification for a plaintext and a signature; or  
7   a process of sharing of a secret key between two parties without  
8   revealing the secret key to a third party.

1           12. An elliptic curve exponentiation method for use in  
 2   an elliptic curve exponentiation apparatus that computes an  
 3   elliptic curve exponentiation for an elliptic curve  $E: y^2 = x^3 + ax + b$   
 4    $\times x + b$  defined over a residue field  $F$  with a prime  $p$  being a  
 5   modulus, and that includes an information obtaining unit,  
 6   a first storage unit storing a coefficient  $a$  that is an  $x$   
 7   term of the elliptic curve  $E$ , a computation unit, a judgment  
 8   unit, and an output unit, the method comprising:  
 9           an information obtaining step, executed by the  
 10   information obtaining unit, of obtaining a point  $Q$  that is  
 11   on the elliptic curve  $E$ , and an exponent  $k$  that is a positive  
 12   integer smaller than the prime  $p$ ;  
 13           a computation step, executed by the computation unit,  
 14   of computing an elliptic curve exponentiation of the exponent  
 15    $k$  and the point  $Q$  using the coefficient  $a$  stored in the first  
 16   storage unit, to obtain an exponentiation-result-point  $k*Q$ ;  
 17           a judgment step, executed by the judgment unit, of judging  
 18   whether the obtained exponentiation-result-point  $k*Q$  is on  
 19   the elliptic curve  $E$ ; and  
 20           an output step, executed by the output unit, of outputting  
 21   the obtained exponentiation-result-point  $k*Q$ , when a judgment  
 22   result in the judging step is affirmative.

1           13. A computer program for computation of an elliptic  
 2   curve exponentiation, for use in an elliptic curve

3    exponentiation apparatus that computes an elliptic curve  
4    exponentiation for an elliptic curve  $E: y^2 = x^3 + a \times x + b$  defined  
5    over a residue field  $F$  with a prime  $p$  being a modulus, and  
6    that includes an information obtaining unit, a first storage  
7    unit storing a coefficient  $a$  that is an  $x$  term of the elliptic  
8    curve  $E$ , a computation unit, a judgment unit, and an output  
9    unit, the program comprising:

10        an information obtaining step, executed by the  
11    information obtaining unit, of obtaining a point  $Q$  that is  
12    on the elliptic curve  $E$ , and an exponent  $k$  that is a positive  
13    integer smaller than the prime  $p$ ;

14        a computation step, executed by the computation unit,  
15    of computing an elliptic curve exponentiation of the exponent  
16     $k$  and the point  $Q$  using the coefficient  $a$  stored in the first  
17    storage unit, to obtain an exponentiation-result-point  $k \times Q$ ;

18        a judgment step, executed by the judgment unit, of judging  
19    whether the obtained exponentiation-result-point  $k \times Q$  is on  
20    the elliptic curve  $E$ ; and

21        an output step, executed by the output unit, of outputting  
22    the obtained exponentiation-result-point  $k \times Q$ , when a  
23    judgment result in the judging step is affirmative.

1        14. The computer program of Claim 13, recorded on a  
2    computer-readable recording medium.